U.S. APPLICATION NO. 09/914172	INTERNATIONAL APPLICATION NO. PCT/FR00/00472	ATTORNEY'S DOCKET NUMBER 98RO21254297

	CALCULATIONS (PTO USE ONLY)	
X 17. The following fees are submitted:		
BASIC NATIONAL FEE (37 CFR 1.492(a)(1)-(5)):		
Search Report has been prepared by the EPO or JPO $860.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) $750.00		
No international preliminary exam fee paid to USPTO but int'l search fee paid to USPTO (37 CFR 1.445(a)(2)) $700.00		
Neither international preliminary examination fee nor int'l search fee (37 CFR 1.445(a)(2)) paid to USPTO $970.00		
International preliminary examination fee paid to USPTO and all claims satisfied provisions of PCT Article 33(2)-(4) $96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$860.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than ____20 ____30 months from the earliest claimed priority date (37 CFR 1.492(e)). **The filing fee has been calculated according to the Preliminary Amendment filed herewith as shown below:**	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	11 - 20 =	0	x $18.00	$	
Independent claims	3 - 3 =	0	x $80.00	$	
MULTIPLE DEPENDENT CLAIM(s) (if applicable)			+ $270.00	$	
TOTAL OF ABOVE CALCULATIONS =				$860.00	
SUBTOTAL =				$860.00	
Processing fee of **$130.00** for furnishing the English translation later than ____20 ____30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$860.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3 28, 3.31). **$40.00** per property +				$900.00	
TOTAL FEES ENCLOSED =				$900.00	
				Amount to be: **refunded**	$
				charged	$

a. X A check in the amount of $ 900.00 to cover the above fees is enclosed.

b. ____ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. X The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 01-0484 .

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

[X] **PLEASE ADDRESS ALL CORRESPONDENCE TO ATTORNEY OF RECORD: CHRISTOPHER F. REGAN**

[X] Associate this file with Customer No. 27975.

27975

PATENT TRADEMARK OFFICE

Michael W. Taylor

SIGNATURE

MICHAEL W. TAYLOR

NAME

43,182

REGISTRATION NUMBER

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
ROMAIN

Serial No. **Not Yet Assigned**

Filing Date: **Herewith**

For: **METHOD FOR PROVIDING SECURITY TO A CHAINING OF OPERATIONS PERFORMED BY AN ELECTRONIC CIRCUIT WITHIN THE CONTEXT OF EXECUTING AN ALGORITHM**

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"EXPRESS MAIL" MAILING LABEL NUMBER EL740059419US

DATE OF DEPOSIT August 24, 2001

I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST OFFICE TO ADDRESSEE" SERVICE UNDER 37 CFR 1.10 ON THE DATE INDICATED ABOVE AND IS ADDRESSED TO THE COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20031

Greg French
(TYPED OR PRINTED NAME OF PERSON MAILING PAPER OR FEE)

(SIGNATURE OF PERSON MAILING PAPER OR FEE)

PRELIMINARY AMENDMENT

Director
U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

Prior to the calculation of fees and examination of the present application, please enter the amendments and remarks set out below.

In the Claims:

Please cancel Claims 1 to 6.

Please add new Claims 7 to 17.

7. A method for providing security to a chaining of useful operations, of a same type, performed by an electronic circuit executing an algorithm, each of the useful operations corresponding to a step of the algorithm, the method comprising:

randomly introducing at least one dummy operation of the same type in the chaining of useful operations.

8. A method according to Claim 7, further comprising maintaining a constant time interval between execution of two successive useful operations.

9. A method according to Claim 7, further comprising maintaining a constant time interval between execution of two successive dummy operations.

10. A method according to Claim 7, further comprising maintaining a constant time interval between execution of two successive useful and dummy operations.

11. A method according to Claim 7, wherein a number of dummy operations is constant for each new execution of the algorithm.

12. A method for providing security to an electronic circuit executing an algorithm, the method comprising:

executing the algorithm so that useful operations of a same type are chained together, with each useful operation corresponding to a step of the algorithm; and

randomly introducing at least one dummy operation of the same type in the chaining of useful operations.

13. A method according to Claim 12, further comprising maintaining a constant time interval between execution of two successive useful operations.

14. A method according to Claim 12, further comprising maintaining a constant time interval between execution of two successive dummy operations.

15. A method according to Claim 12, further comprising maintaining a constant time interval between execution of two successive useful and dummy operations.

16. A method according to Claim 12, wherein a number of dummy operations is constant for each new execution of the algorithm.

17. An electronic device comprising:

a processor for executing an algorithm that includes a plurality of useful operations of a same type, and a routine for providing security to a chaining of the plurality of useful operations, with each useful operation corresponding to a step of the algorithm, the routine randomly introducing at least one dummy operation of the same type in the chaining of useful operations.

18. An electronic device according to Claim 17, wherein the routine maintains a constant time interval between execution of two successive useful operations.

19. An electronic device according to Claim 17, wherein the routine maintains a constant time interval between execution of two successive dummy operations.

20. An electronic device according to Claim 17, wherein the routine maintains a constant time interval between execution of two successive useful and dummy operations.

21. An electronic device according to Claim 17, wherein a number of dummy operations is constant for each new

execution of the algorithm.

22. An electronic device according to Claim 17, wherein the electronic device is configured as a chip card.

REMARKS

It is believed that all of the claims are patentable over the prior art. For better readability and the Examiner's convenience, the newly submitted claims differ from the translated counterpart claims which are being canceled. The newly submitted claims do not represent changes or amendments that narrow the claim scope for any reason related to the statutory requirements for patentability. Accordingly, after the Examiner completes a thorough examination and finds the claims patentable, a Notice of Allowance is respectfully requested in due course. Should the Examiner determine any minor informalities that need to be addressed, he is encouraged to contact the undersigned attorney at the telephone number below.

Respectfully submitted,

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Applicant

SUBSTITUTE SPECIFICATION

METHOD FOR PROVIDING SECURITY TO A CHAINING OF OPERATIONS PERFORMED BY AN ELECTRONIC CIRCUIT WITHIN THE CONTEXT OF EXECUTING AN ALGORITHM

Field of the Invention

The present invention relates to the field of cryptology, and more particularly, to a method for providing security to a chaining of operations performed by an electronic circuit executing an algorithm. In the context of the invention, an algorithm should be understood as a chaining of actions required for accomplishing a task. Therefore, this does not necessarily mean the implementation of a computer program.

Background of the Invention

Cryptology may be defined as the science for hiding information. It forms with the physical security of the components and operating systems the essential dimension of security for chip cards. Cryptology includes cryptography which is the art of encrypting and decrypting messages, and cryptological analysis which is the art of breaking secret codes.

In chip cards, cryptography implements various mechanisms which have the purpose of providing either confidentiality of the information, or

authentication of the cards or the users, or even the signature of messages. All the means which implement cryptography form a cryptosystem. Such cryptosystems contain confidential information, notably for encryption and decryption of digital messages.

Among this confidential information, the encryption and decryption keys which are parameters of a secret agreement used for encryption and decryption of digital messages may be mentioned. The use of these encryption and decryption keys often requires several data transfers which characterizes them. When they are used within a cryptosystem, the characteristic data of digital keys and other confidential information flow between various memory or processing registers and modules. These transfers between registers and/or modules are expressed by the appearance of electrical currents or magnetic fields bearing pieces of confidential information. These pieces of confidential information may for example, relate to the encryption and decryption keys.

Such cryptosystems pose a problem of visibility from the outside world. A measurement of the electrical signals or the magnetic fields arising from the exchanges of information between different portions of the circuit may provide access to pieces of confidential information which are involved in the protection of data by the encryption or decryption system. For example, one of the electrical signals may be located at the power supply contact of the circuit, whether the latter is internal or external.

When the digital key is used by an authorized component, such as a chip card, a certain visibility, for example on the digital key, is made possible by

investigating such electrical signals. The sensitive electrical signals may be observed on different contacts of the circuit, notably connecting different memory or processing registers or modules.

A digital key may thus be discovered as a result of accumulating electrical or magnetic signal measurements and of a statistical analysis of these measurements. More generally, any electronic circuit has an electrical consumption related to the operations which it carries out. It is possible to discover hidden information in the circuit by measuring this consumption. This problem is posed in any secured component, and notably in components for chip cards.

Discovery of protected data by observation of the current generally requires a reproducibility of the current measurement to carry out statistical processing. Thus, when an electronic circuit executes an algorithm containing identical or similar and recurrent operations, such as transfer of confidential data between registers, and where fine observation of the operations one by one may disclose confidential information, a statistical analysis based on the measurement of the aforementioned electrical currents may be detrimental to the security of the electronic circuit.

Summary of the Invention

An object of the present invention is to find a remedy to the problems which have just been described. Accordingly, a method for avoiding a disclosure by observation of the current of protected data is provided. For this purpose, the method for providing security to a chaining of operations

performed by an electronic circuit executing an algorithm provides invisibility with regards to analysis of electrical signals related to data transfers between various registers. More specifically, the security is provided by the presence of parasitic information which interferes with the observation, from the outside of the electronic circuit, of physical phenomena associated with the execution of useful operations.

To achieve this object, the invention inserts dummy operations in a chaining of useful operations of the same type, which is carried out in the context of executing an algorithm. The dummy operations are very similar to the useful operations. Each dummy operation is inserted at a random line for each execution of the algorithm. Thus, acquisition of comparable current measurements becomes very difficult.

A dummy operation may be designed as an operation having an identical signature or virtually very close to a useful operation in terms of the observable physical parameters associated with the execution of this instruction (e.g., current consumption, magnetic radiation, etc.). These physical parameters may notably be detected at a current or voltage supply terminal of the circuit. In this way, the present dummy operations cannot be detected, sample by sample, and therefore they prevent any statistical analysis or at least make it very difficult.

The invention accordingly relates to a method for providing security to a chaining of useful operations, of the same type, performed by an electronic circuit in the context of executing an algorithm. Each of the useful operations corresponds

to a step of the algorithm, characterized in that the method comprises randomly introducing one or several dummy operations of the same type in the chaining of useful operations.

A dummy operation of the same type as a useful operation may assume various forms according to the relevant application, from the moment that it has physical characteristics which appear identical or sufficiently close to a useful operation to make its detection difficult. As a non-limiting example, a dummy operation may be the real execution of a calculation, but without recording the result in memory, or with recording but in an inoperative memory for the relevant operation.

False calculations or false subsets of operations may thus be introduced with the dummy operations. The present invention also relates to an electronic device for executing an algorithm, for example a chip card, characterized in that it implements the aforementioned method for providing security, possibly with the optional aspects which are described below.

Various aspects and advantages of the invention will become more clearly apparent in the following description, which shows a preferred embodiment of the method according to the invention and which is only given indicatively and by no means as limiting the invention.

Detailed Description of the Preferred Embodiments

According to a preferred embodiment of the invention, a certain number of dummy operations are inserted between useful operations, of the same type,

performed by an electronic circuit executing an algorithm. These dummy operations are introduced in a random way, and may be introduced in any useful operation associated with the algorithm.

One or several dummy operations may also be found before the first useful operation associated with an algorithm, or after the last useful operation associated with an algorithm. Several consecutive dummy operations may also be found. To provide different series of current measurements at each execution of a same algorithm, new random operations are introduced in each execution of an algorithm.

However, in a preferred application, the method according to the invention comprises the additional step of maintaining a constant time interval between the performance of two operations, whether they are successive useful and/or dummy operations. Thus, the insertion of dummy operations does not obviously appear upon a time investigation of the electrical signals associated with the useful operations performed by an electronic circuit in the context of executing an algorithm.

Finally, it is preferable but not mandatory that the number of dummy operations introduced in the chaining of useful operations be constant for each new execution of the algorithm. Thus, the execution time of the algorithm in its whole is the same for each execution of the algorithm. The fact that dummy operations have been introduced is thus invisible upon a first analysis, which again provides better security for the chaining of useful operations.

According to the invention, it is also possible to distribute the random operations only on

certain portions of the algorithm. Further, the method according to invention may also be applied to algorithms having operations which are ordered, i.e., the useful operations must be chained in an order which cannot be changed. The number of introduced dummy operations in a preferred application of the invention is on the order of 2 percent based on the total number of performed operations.

THAT WHICH IS CLAIMED IS:

1. A method for providing security to a chaining of useful operations, of the same type, performed by an electronic circuit in the context of executing an algorithm, each of the useful operations corresponding to a step of the algorithm, characterized in that the method comprises the step consisting of introducing randomly one or several dummy operations of the same type in the chaining of operations.

2. The method for providing security to a chaining of operations of the same type, according to claim 1, characterized in that the method comprises the additional step consisting of keeping a constant time interval between the performance of two successive useful and/or dummy operations.

3. The method for providing security to a chaining of operations of the same type, according to any of claims 1 or 2, characterized in that the number of dummy operations introduced in the chaining of operations is constant for each new execution of the algorithm.

4. A use of the method according to any of the preceding claims, in the field of cryptography.

5. An electronic device for executing an algorithm, characterized in that it implements the method for providing security according to any of claims 1 to 3.

6. A chip card comprising an electronic device for executing an algorithm, characterized in that it implements the method for providing security according to any of claims 1 to 3.

METHOD FOR PROVIDING SECURITY TO A CHAINING OF OPERATIONS PERFORMED BY AN ELECTRONIC CIRCUIT WITHIN THE CONTEXT OF EXECUTING AN ALGORITHM

Abstract of the Disclosure

A method for providing security to a chaining of useful operations of the same type, performed by an electronic circuit executing an algorithm, randomly introduces one or more dummy operations in the chaining of operations. This prevents any fraudulent access to protected data through a statistical analysis of electric currents.

SUBSTITUTE SPECIFICATION

METHOD FOR PROVIDING SECURITY TO A CHAINING OF OPERATIONS PERFORMED BY AN ELECTRONIC CIRCUIT WITHIN THE CONTEXT OF EXECUTING AN ALGORITHM

Field of the Invention

The present invention relates to the field of cryptology, and more particularly, to a method for providing security to a chaining of operations performed by an electronic circuit ~~in the context of~~ executing an algorithm.

~~More specifically, the invention relates to a method for providing security to an chaining of useful operations of the same type, performed by an electronic circuit in the context of executing an algorithm, the security being provided by the presence of parasitic information which interferes with the observation, from the outside of the electronic circuit, of physical phenomena associated with the execution of useful operations.~~

In the context of the invention, an algorithm should be understood as a chaining of actions required for accomplishing a task. Therefore, this does not necessarily mean the implementation of a computer program.

~~The field of application of the invention, is essentially the field of cryptology.~~

Background of the Invention

Cryptology may be defined as the science for hiding information. It forms with the physical security of the components and operating systems~~,~~ the essential dimension of security for chip cards. Cryptology includes cryptography which is the art ~~for encryption~~of encrypting and ~~decryption~~decrypting messages, and cryptological analysis which is the art of breaking secrete codes.

In chip cards, cryptography implements various mechanisms which have the purpose of providing either confidentiality of the information, or authentication of the cards or the users, or even the signature of messages.

All the means which implement cryptography form a cryptosystem. Such cryptosystems contain confidential information, notably for encryption and decryption of digital messages.

Among this confidential information, the encryption and decryption keys which are parameters of a secret agreement used for encryption and decryption of digital messages may be mentioned.

The use of these encryption and decryption keys often requires several data transfers which characterizes them. When they are used within a cryptosystem, the characteristic data of digital keys and other confidential information flow between various memory or processing registers and modules. These transfers between registers and/or modules are expressed by the appearance of electrical currents or magnetic fields bearing pieces of confidential information. These pieces of confidential information

may for example, relate to the encryption and decryption keys.

Such cryptosystems pose a problem of visibility from the outside world. ~~Indeed, a~~ A measurement of the electrical signals or the magnetic fields arising from the exchanges of information between different portions of the circuit may provide access to pieces of confidential information which are involved in the protection of data by the encryption or decryption system.

~~———————~~ For example, one of the electrical signals may be located at the power supply contact of the circuit, whether the latter is internal or external.

~~Indeed, w~~When the digital key is used by an authorized component, such as a chip card, a certain visibility, for example, on the digital key, is made possible by investigating such electrical signals. The sensitive electrical signals may be observed on different contacts of the circuit, notably connecting different memory or processing registers or modules.

A digital key may thus be discovered as a result of accumulating electrical or magnetic signal measurements and of a statistical analysis of these measurements.

~~———————~~ More generally, any electronic circuit has an electrical consumption related to the operations which it carries out. It is possible to discover hidden information in the circuit by measuring this consumption. This problem is posed in any secured component, and notably in components for chip cards.

Discovery of protected data by observation of the current, generally requires a reproducibility of

the current measurement ~~in order~~ to carry out statistical processing.

Thus, when an electronic circuit executes an algorithm containing identical or similar and recurrent operations, such as transfer of confidential data between registers, and where fine observation of the operations one by one may disclose confidential information, a statistical analysis based on the measurement of the aforementioned electrical currents may be detrimental to the security of the electronic circuit.

Summary of the ~~electronic circuit.~~ Invention

~~The~~An object of the present invention is to find a remedy to the problems which have just been described.

Accordingly, ~~the invention provides~~ a method for avoiding a disclosure by observation of the current~~,~~ of protected data is provided.

For this purpose, the ~~invention provides a~~ method for providing security to a chaining of operations performed by an electronic circuit ~~in the context of~~ executing an algorithm ~~which~~ provides invisibility with regards to analysis of electrical signals ~~upon~~related to data transfers between various registers. More specifically, the security is provided by the presence of parasitic information which interferes with the observation, from the outside of the electronic circuit, of physical phenomena associated with the execution of useful operations.

To achieve ~~these~~this objects, the invention ~~provides insertion of~~inserts dummy operations in a chaining of useful operations of the same type, which

is carried out in the context of executing an algorithm. The dummy operations are very similar to the useful operations. Each dummy operation is inserted at a random line for each execution of the algorithm. Thus, acquisition of comparable current measurements becomes very difficult.

A dummy operation may be designed as an operation having an identical signature or virtually very close to a useful operation in terms of the observable physical parameters associated with the execution of this instruction (e.g., current consumption, magnetic radiation, etc.). These physical parameters may notably be detected at a current or voltage supply terminal of the circuit. In this way, the present dummy operations cannot be detected, sample by sample, and therefore they prevent any statistical analysis or at least make it very difficult.

The invention accordingly relates to a method for providing security to a chaining of useful operations, of the same type, performed by an electronic circuit in the context of executing an algorithm~~, e~~. Each of the useful operations ~~corresponding~~corresponds to a step of the algorithm, characterized in that the method comprises ~~the step consisting of~~ randomly introducing one or several dummy operations~~,~~ of the same type in the chaining of useful operations.

A dummy operation of the same type as a useful operation may assume various forms according to the relevant application, from the moment that it has physical characteristics which appear identical or sufficiently close to a useful operation ~~in order~~ to make its detection difficult. As a non-limiting

example, a dummy operation may be the real execution of a calculation, but without recording the result in memory, or with recording but in an inoperative memory for the relevant operation.

False calculations or false subsets of operations may thus be introduced with the dummy operations.

The present invention also relates to an electronic device for executing an algorithm, for example a chip card, characterized in that it implements the aforementioned method for providing security, possibly with the optional aspects which are described ~~in what follows~~below.

Various aspects and advantages of the invention will become more clearly apparent in the following description, which shows a preferred embodiment of the method according to the invention and which is only given indicatively and by no means as limiting the invention.

Detailed Description of the Preferred Embodiments

According to a preferred embodiment of the invention, a certain number of dummy operations are inserted between useful operations, of the same type, performed by an electronic circuit ~~in the context of~~ executing an algorithm. These dummy operations are introduced in a random way~~: these dummy operations~~, and may be introduced in any useful operation associated with the algorithm.

One or several dummy operations may also be found before the first useful operation associated with an algorithm, or after the last useful operation

associated with an algorithm. Several consecutive dummy operations may also be found.

~~In order t~~ To provide different series of current measurements at each execution of a same algorithm, new random operations are introduced in each execution of an algorithm.

However, in a preferred application, the method according to the invention comprises the additional step ~~consisting~~ of maintaining a constant time interval between the performance of two operations, whether they are successive useful and/or dummy operations. Thus, the insertion of dummy operations does not obviously appear upon a time investigation of the electrical signals associated with the useful operations performed by an electronic circuit in the context of executing an algorithm.

Finally, it is preferable but not mandatory that the number of dummy operations introduced in the chaining of useful operations be constant for each new execution of the algorithm. Thus, the execution time of the algorithm in its whole is the same for each execution of the algorithm. The fact that dummy operations have been introduced is thus invisible upon a first analysis, which again provides better security for the chaining of useful operations.

According to the invention, it is also possible to distribute the random operations only on certain portions of the algorithm. Further, the method according to invention may also be applied to algorithms~~, the~~ having operations ~~of~~ which are ordered, i.e., the useful operations must be chained in an order which cannot be changed.

The number of introduced dummy operations in a preferred application of the invention is of the order of 2 percent based on the total number of performed operations.

~~CLAIMS~~**THAT WHICH IS CLAIMED IS:**

1. A method for providing security to a chaining of useful operations, of the same type, performed by an electronic circuit in the context of executing an algorithm, each of the useful operations corresponding to a step of the algorithm, characterized in that the method comprises the step consisting of introducing randomly one or several dummy operations of the same type in the chaining of operations.

2. The method for providing security to a chaining of operations of the same type, according to claim 1, characterized in that the method comprises the additional step consisting of keeping a constant time interval between the performance of two successive useful and/or dummy operations.

3. The method for providing security to a chaining of operations of the same type, according to any of claims 1 or 2, characterized in that the number of dummy operations introduced in the chaining of operations is constant for each new execution of the algorithm.

4. A use of the method according to any of the preceding claims, in the field of cryptography.

5. An electronic device for executing an algorithm, characterized in that it implements the method for providing security according to any of claims 1 to 3.

6. A chip card comprising an electronic device for executing an algorithm, characterized in that it implements the method for providing security according to any of claims 1 to 3.

~~ABSTRACT OF THE DISCLOSURE~~

METHOD FOR PROVIDING SECURITY TO A CHAINING OF OPERATIONS PERFORMED BY AN ELECTRONIC CIRCUIT WITHIN THE CONTEXT OF EXECUTING AN ALGORITHM

Abstract of the Disclosure

~~The invention relates to a~~ A method for providing security to a chaining of useful operations of the same type, performed by an electronic circuit ~~in the context of~~ executing an algorithm~~. The method according to the invention involves a step consisting of~~, randomly ~~introducing~~introduces one or ~~several~~more dummy operations in the chaining of operations~~, in order to~~. This prevents any fraudulent access~~,~~ to protected data through a statistical analysis of electric currents~~, to protected data~~.

METHOD FOR PROVIDING SECURITY TO A CHAINING OF OPERATIONS PERFORMED BY AN ELECTRONIC CIRCUIT WITHIN THE CONTEXT OF EXECUTING AN ALGORITHM

The present invention relates to a method for providing security to a chaining of operations performed by an electronic circuit in the context of executing an algorithm.

More specifically, the invention relates to a method for providing security to an chaining of useful operations of the same type, performed by an electronic circuit in the context of executing an algorithm, the security being provided by the presence of parasitic information which interferes with the observation, from the outside of the electronic circuit, of physical phenomena associated with the execution of useful operations.

In the context of the invention, an algorithm should be understood as a chaining of actions required for accomplishing a task. Therefore, this does not necessarily mean the implementation of a computer program.

The field of application of the invention, is essentially the field of cryptology. Cryptology may be

defined as the science for hiding information. It forms with the physical security of the components and operating systems, the essential dimension of security for chip cards. Cryptology includes cryptography which is the art for encryption and decryption messages and cryptological analysis which is the art of breaking secrete codes.

In chip cards, cryptography implements various mechanisms which have the purpose of providing either confidentiality of the information, or authentication of the cards or the users, or even the signature of messages.

All the means which implement cryptography form a cryptosystem. Such cryptosystems contain confidential information, notably for encryption and decryption of digital messages.

Among this confidential information, the encryption and decryption keys which are parameters of a secret agreement used for encryption and decryption of digital messages may be mentioned.

The use of these encryption and decryption keys often requires several data transfers which characterize them. When they are used within a cryptosystem, the characteristic data of digital keys and other confidential information flow between various memory or processing registers and modules. These transfers between registers and/or modules are expressed by the appearance of electrical currents or magnetic fields bearing pieces of confidential information. These pieces of confidential information may for example, relate to the encryption and decryption keys.

Such cryptosystems pose a problem of visibility

from the outside world. Indeed, a measurement of the electrical signals or the magnetic fields arising from the exchanges of information between different portions of the circuit may provide access to pieces of confidential information which are involved in the protection of data by the encryption or decryption system.

For example, one of the electrical signals may be located at the power supply contact of the circuit, whether the latter is internal or external.

Indeed, when the digital key is used by an authorized component, such as a chip card, a certain visibility for example, on the digital key, is made possible by investigating such electrical signals. The sensitive electrical signals may be observed on different contacts of the circuit, notably connecting different memory or processing registers or modules.

A digital key may thus be discovered as a result of accumulating electrical or magnetic signal measurements and of a statistical analysis of these measurements.

More generally, any electronic circuit has an electrical consumption related to the operations which it carries out. It is possible to discover hidden information in the circuit by measuring this consumption. This problem is posed in any secured component and notably in components for chip cards.

Discovery of protected data by observation of the current, generally requires a reproducibility of the current measurement in order to carry out statistical processing.

Thus, when an electronic circuit executes an algorithm containing identical or similar and recurrent

operations, such as transfer of confidential data between registers, and where fine observation of the operations one by one may disclose confidential information, a statistical analysis based on the measurement of the aforementioned electrical currents may be detrimental to the security of the electronic circuit.

The object of the present invention is to find a remedy to the problems which have just been described.

Accordingly, the invention provides a method for avoiding a disclosure by observation of the current, of protected data.

For this purpose, the invention provides a method for providing security to a chaining of operations performed by an electronic circuit in the context of executing an algorithm which provides invisibility with regards to analysis of electrical signals upon data transfers between various registers.

To achieve these objects, the invention provides insertion of dummy operations in a chaining of useful operations of the same type, carried out in the context of executing an algorithm. The dummy operations are very similar to the useful operations. Each dummy operation is inserted at a random line for each execution of the algorithm. Thus, acquisition of comparable current measurements becomes very difficult.

A dummy operation may be designed as an operation having an identical signature or virtually very close to a useful operation in terms of the observable physical parameters associated with the execution of this instruction (current consumption, magnetic radiation, etc.). These physical parameters may notably be detected at a current or voltage supply terminal of

the circuit. In this way, the present dummy operations cannot be detected, sample by sample, and therefore they prevent any statistical analysis or at least make it very difficult.

The invention accordingly relates to a method for providing security to a chaining of useful operations, of the same type, performed by an electronic circuit in the context of executing an algorithm, each of the useful operations corresponding to a step of the algorithm, characterized in that the method comprises the step consisting of randomly introducing one or several dummy operations, of the same type in the chaining of useful operations.

A dummy operation of the same type as a useful operation may assume various forms according to the relevant application, from the moment that it has physical characteristics which appear identical or sufficiently close to a useful operation in order to make its detection difficult. As a non-limiting example, a dummy operation may be the real execution of a calculation, but without recording the result in memory, or with recording but in an inoperative memory for the relevant operation.

False calculations or false subsets of operations may thus be introduced with the dummy operations.

The present invention also relates to an electronic device for executing an algorithm, for example a chip card, characterized in that it implements the aforementioned method for providing security, possibly with the optional aspects which are described in what follows.

Various aspects and advantages of the invention will become more clearly apparent in the following

description, which shows a preferred embodiment of the method according to the invention and which is only given indicatively and by no means as limiting the invention.

According to a preferred embodiment of the invention, a certain number of dummy operations are inserted between useful operations, of the same type, performed by an electronic circuit in the context of executing an algorithm. These dummy operations are introduced in a random way: these dummy operations may be introduced in any useful operation associated with the algorithm.

One or several dummy operations may also be found before the first useful operation associated with an algorithm or after the last useful operation associated with an algorithm. Several consecutive dummy operations may also be found.

In order to provide different series of current measurement at each execution of a same algorithm, new random operations are introduced in each execution of an algorithm.

However, in a preferred application, the method according to the invention comprises the additional step consisting of maintaining a constant time interval between the performance of two operations, whether they are successive useful and/or dummy operations. Thus, the insertion of dummy operations does not obviously appear upon a time investigation of the electrical signals associated with the useful operations performed by an electronic circuit in the context of executing an algorithm.

Finally, it is preferable but not mandatory that the number of dummy operations introduced in the

chaining of useful operations be constant for each new execution of the algorithm. Thus, the execution time of the algorithm in its whole is the same for each execution of the algorithm. The fact that dummy operations have been introduced is thus invisible upon a first analysis, which again provides better security for the chaining of useful operations.

According to the invention, it is also possible to distribute the random operations only on certain portions of the algorithm. Further, the method according to invention may also be applied to algorithms, the operations of which are ordered i.e. the useful operations must be chained in an order which cannot be changed.

The number of introduced dummy operations in a preferred application of the invention is of the order of 2 percent based on the total number of performed operations.

CLAIMS

1. A method for providing security to a chaining of useful operations, of the same type, performed by an electronic circuit in the context of executing an algorithm, each of the useful operations corresponding to a step of the algorithm, characterized in that the method comprises the step consisting of introducing randomly one or several dummy operations of the same type in the chaining of operations.

2. The method for providing security to a chaining of operations of the same type, according to claim 1, characterized in that the method comprises the additional step consisting of keeping a constant time interval between the performance of two successive useful and/or dummy operations.

3. The method for providing security to a chaining of operations of the same type, according to any of claims 1 or 2, characterized in that the number of dummy operations introduced in the chaining of operations is constant for each new execution of the algorithm.

4. A use of the method according to any of the preceding claims, in the field of cryptography.

5. An electronic device for executing an algorithm, characterized in that it implements the method for providing security according to any of claims 1 to 3.

6. A chip card comprising an electronic device for executing an algorithm, characterized in that it implements the method for providing security according to any of claims 1 to 3.

ABSTRACT OF THE DISCLOSURE

METHOD FOR PROVIDING SECURITY TO A CHAINING OF OPERATIONS PERFORMED BY AN ELECTRONIC CIRCUIT WITHIN THE CONTEXT OF EXECUTING AN ALGORITHM

The invention relates to a method for providing security to a chaining of useful operations of the same type, performed by an electronic circuit in the context of executing an algorithm. The method according to the invention involves a step consisting of randomly introducing one or several dummy operations in the chaining of operations, in order to prevent any fraudulent access, through a statistical analysis of electric currents, to protected data.

FR04259 "27 1 1 1

014415 / PC/US

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

Attorney Docket No.: **98RO21254297**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **METHOD FOR PROVIDING SECURITY TO A CHAINING OF OPERATIONS PERFORMED BY AN ELECTRONIC CIRCUIT WITHIN THE CONTEXT OF EXECUTING AN ALOGORITHM**, the specification of which:

(check one)

__X__ is attached hereto

_____ was filed on _____

as Application Serial No. _____

and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulation, 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the of the application on which priority is claimed:

Prior Foreign Application(s) Priority Claimed

(Number)	(Country)	(Day/Month/Year Filed)	[X] Yes	[ ] No
99/02364	FR	25 February 1999		
			[ ] Yes	[ ] No
			[ ] Yes	[ ] No

I hereby claim the benefit under Title 35, United States Code, 120, of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Appln Serial No.)	(Filing Date)	(Status) (patented, pending, aban.)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

English Language Declaration

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: **Christopher F. Regan**, Reg. No. 34,906; **Herbert L. Allen**, Reg. No. 25,322; **David L. Sigalow**, Reg. No. 36,006; **Jeffrey S. Whittle**, Reg. No. 36,382; **Richard K. Warther**, Reg. No. 32,180; **Michael W. Taylor**, Reg. No. 43,182; **Henry Estevez**, Reg. No. 37,823; **Paul J. Ditmyer**, Reg. No. 40,455; **John F. Woodson, II**, Reg. No. 45,236; **Charles E. Wands**, Reg. No. 25,649; **Jacqueline E. Hartt**, Reg. No. 37,845; **Mark R. Malek**, Reg. No. 46,894; **Richard A. Hinson**, Reg. No. 47,652 and **Theodore E. Galanthay**, Reg. No. 24,122. (14)

Send Correspondence to:

CHRISTOPHER F. REGAN, ESQUIRE
ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST, P.A.
P.O. Box 3791
Orlando, Florida 32802-3791

Direct Telephone Calls to:

Christopher F. Regan
(407) 841-2330

Full name of inventor: **Fabrice ROMAIN**

Inventor's Signature: FABRICE ROMAIN Date: August, 16th 2001

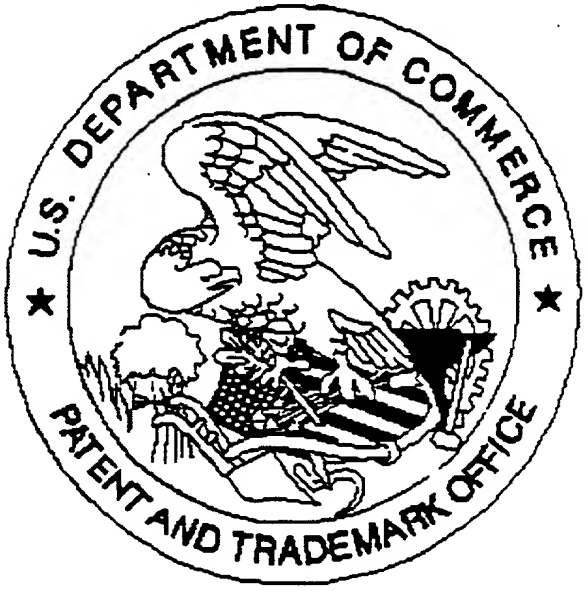
Residence: **Aix En Provence, France**

Citizenship: **Citizen of France**

Mailing Address: **Les Héliades - Bâtiment A**
535, avenue de Bagatelle
13090 Aix En Provence, France FR

United States Patent & Trademark Office

Office of Initial Patent Examination -- Scanning Division



Application deficiencies found during scanning:

☑ Page(s) 1 of 2 of Transmittal were not present for scanning. (Document title)

☐ Page(s)_____ of_____ were not present for scanning. (Document title)

☐ ***Scanned copy is best available.***